

Ste citliví na ochranu údajov? Tento prehľad je niečo ako povinné čítanie pre občanov a odborníkov

- Ako sa európske krajiny vyrovnávajú so špehovacím zákonom
- Odporúčania Európskeho výboru pre ochranu údajov
- Všetko zlé je na niečo dobré a naopak
- Už keď máme lex korona, na čo nezabudnúť

Eurokomisár telefonuje operátorom

Thierry Breton, európsky komisár pre vnútorný trh, usporiadal [konferenčný hovor](#) so vrcholnými zástupcami európskych telekomunikačných spoločností a združením mobilných operátov GSMA. V mene Európskej komisie vyzval európske telekomunikačné giganty ako Deutsche Telekom a Orange, aby **zdieľali mobilné dáta osôb z celého regiónu** s cieľom pomôcť pri predpovedaní šírenia koronavírusu. Dáta by mali byť odovzdávané v agregovanej a anonymizovanej podobe. Takýto zber dát by mali ideálne poskytovať najväčší prevádzkovatelia mobilných služieb v krajinách.

Európska komisia trvala na tom, aby sa pri operácii dodržiavali pravidlá ochrany súkromia v zmysle GDPR a smernice o elektronickom súkromí. Očakávanie by sa dalo stručne popísať ako - Európska komisia nevyžaduje ultimatívne vedieť a vyhodnocovať, či občania dodržiavajú nariadenia jednotlivých vlád. Zaujímajú ju dáta v agregovanej podobe na predikovanie šírenia vírusu, ktoré sa robí aj na základe klesajúcej alebo rastúcej mobility osôb.

Povinné selfies v karanténe alebo iba zdvorilé rady?

Nemecko, Francúzsko, Taliansko aj Slovensko zmenili a doplnili svoje [právne predpisy](#) s cieľom umožniť spracovanie osobných údajov v prípade epidémie. Zákomom sa dostalo nelichotivého označenia ako *špehovacie* a na druhej strane u časti (aj odbornej) verejnosti nadšených ovácií. Takže – kde je pravda? Ako zvyčajne, niekde v strede.

- Telekomunikační operátori začali v mnohých európskych krajinách poskytovať údaje o pohybe občanov.
- Vo Francúzsku sa vďaka zmene legislatívy požaduje, aby zákonodarcovia zhromažďovali telekomunikačné údaje po dobu šiestich mesiacov.
- Anonymizované údaje o občanoch sa zbierajú aj v Belgicku po dobu troch mesiacov.
- Nemecký mobilný operátor Deutsche Telekom zdieľa anonymné údaje o pohybe používateľov s inštitútom Robert-Koch. Dáta sa používajú na zistenie, či ľudia v dôsledku pandémie dodržiavajú vládne obmedzenia.
- V Taliansku spoločnosť Vodafone pripravuje súhrnnú a anonymnú tepelnú mapu o pohybe občanov pre Lombardsko, aby pomohla orgánom lepšie porozumieť pohybom obyvateľstva.

- Spoločnosť Vodafone poskytuje podobné informácie aj o pohybe obyvateľstva v Španielsku.
- Rakúsky mobilný operátor A1 Telekom Austria poskytuje zdravotníckym autoritám výsledky z aplikácie, ktorá vizualizuje pohybové aktivity obyvateľstva. Rakúsky Červený kríž spustil aplikáciu *Stop Corona*, ktorej stiahnutie je dobrovoľné. Aplikácia umožňuje používateľovi vytvárať si zoznam osôb, s ktorými sa stretol. Ak niektorá z týchto osôb ochorie, používateľ aplikácie bude o tejto skutočnosti upovedomený.
- Česká republika plánuje spustiť tzv. inteligentnú karanténu, ktorá pomocou dát z mobilných telefónov a platobných kariet umožní zmapovať, kde sa nakazená osoba pohybovala posledných päť dní.
- Niektoré praktiky krajín sú už na hranici zákonnosti. V Poľsku bola zavedená aplikácia pod názvom *Home Quarantine*, ktorá vyžaduje od ľudí v povinnej karanténe fotenie selfies aj s uvedením ich aktuálnej polohy. Na nahrávanie fotografií ich vyzývajú SMS správy. Kto nemá stiahnutú aplikáciu, môže očakávať fyzické kontroly dodržiavania karantény.

Nech už nazývate smernicu GDPR akokoľvek (zbytočná administratíva, postrach, nástroj na pokuty), jej cieľom je presne to, čo má obsiahnuté v názve – Nariadenie EÚ o všeobecnej ochrane údajov (General Data Protection Regulation – GDPR) Toto nariadenie však umožňuje dočasné pozastavenie niektorých práv na ochranu údajov v čase krízy, akou je momentálne pandémie koronavírusu v roku 2020.

Či už ste dátový odborník alebo občan, ktorému záleží na stave spoločnosti a efektívnom narábaní s jeho dátami, mali by ste vedieť, ako vás chráni európska legislatíva.

Takže dve časti pre tých, ktorým záleží na budúcnosti kybernetickej bezpečnosti.

Vyhlásenie o spracovaní osobných údajov v súvislosti s prepuknutím ochorenia COVID-19

Európsky výbor pre ochranu údajov (EDPB)

19. marca 2020 (prehľad)

Pokiaľ ide o spracovanie osobných údajov vrátane osobitných kategórií údajov príslušnými verejnými orgánmi (napr. orgánmi verejného zdravotníctva), EDPB sa domnieva, že články 6 a 9 GDPR umožňujú spracovanie osobných údajov, najmä ak sa na ne vzťahuje zákonný mandát orgánu verejnej moci.

V prípade spracovania telekomunikačných údajov, ako sú lokalizačné údaje, musia byť dodržané aj vnútroštátne právne predpisy, ktorými sa vykonáva smernica o elektronickom súkromí (ePrivacy Directive).

Údaje o polohe môže prevádzkovateľ v zásade používať iba vtedy, ak sú anonymné alebo so súhlasom jednotlivcov.

Článok 15 smernice o elektronickom súkromí umožňuje členským štátom zaviesť legislatívne opatrenia na zabezpečenie verejnej bezpečnosti. Takáto výnimočná legislatíva je možná iba vtedy, ak predstavuje potrebné, primerané opatrenie v demokratickej spoločnosti.

Verejné orgány by sa mali najprv snažiť spracovať údaje o polohe anonymným spôsobom, tak aby jednotlivci nemohli byť opätovne identifikovaní. Takto spracované údaje by generovali správy o koncentrácii mobilných zariadení na určitom mieste. Pravidlá ochrany osobných údajov sa totiž nevzťahujú na údaje, ktoré boli **primerane anonymizované**.

Ak nie je možné spracovať iba anonymné údaje, smernica o elektronickom súkromí umožňuje členskému štátu zaviesť legislatívne opatrenia na ochranu verejnej bezpečnosti (čl. 15). V takomto prípade je členský štát povinný zaviesť primerané záruky, napríklad poskytnutie práva jednotlivcom na opravný prostriedok pre oblasť elektronických komunikačných služieb.

Možné dosahy legislatívnych opatrení zavedených v čase krízy pre používanie osobných údajov fyzických osôb.

Ohrozenie

- Enormné množstvo zozbieraných údajov
- Čo sa stane so zberom po ukončení krízy
- Navrátenie k opätovnému dodržiavaniu GDPR

Prínos

- Vymedzenie rozsahu legislatívneho opatrenia zavádzajúce zmeny v dobe krízy
- Primerané záruky pre jednotlivca
- Uprednostnenie anonymizovaného spôsobu zberu dát

Kým začnete ohnivo diskutovať, tu je kvalitná munícia

Nariadenie EÚ o všeobecnej ochrane údajov (General Data Protection Regulation – GDPR) umožňuje dočasné pozastavenie niektorých práv na ochranu údajov v čase krízy, akou je momentálne pandémie koronavírusu v roku 2020.

Hlavným cieľom GDPR je ochrana osobných údajov dotknutej osoby, keď použitie vrátane ich prenosu je obmedzené právami dotknutej osoby. Avšak tieto práva nie sú bezpodmienečné a tvorcovia nariadenia predpokladali, že **v prípade občianskej krízy** môžu byť niektoré z práv pozastavené alebo obmedzené.

[The eData Guide To GDPR](#)

V nariadení GDPR sú ustanovené **právne dôvody**, ktoré zamestnávateľom a príslušným orgánom verejného zdravotníctva umožňujú spracovávať osobné údaje v súvislosti s epidémiami bez toho, aby bolo potrebné získať súhlas dotknutej osoby. Platí to napríklad vtedy, keď je spracovanie osobných údajov potrebné pre zamestnávateľov z dôvodov verejného záujmu v oblasti verejného zdravia alebo na ochranu životne dôležitých záujmov (články 6 a 9 GDPR) alebo na splnenie inej zákonnej povinnosti.

[Statement by the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak](#)

Článkom 9 ods. 1 nariadenia GDPR **sa zakazuje spracúvanie osobných údajov**, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov, údajov týkajúcich sa zdravia alebo sexuálneho života a sexuálnej orientácie fyzickej osoby.

Najdôležitejším je článok 9 ods. 2 písm. i, ktorý **umožňuje spracovanie osobných údajov** fyzickej osoby potrebných pre zachovanie verejného zdravia, napríklad aj v prípade ochrany zdravia pred závažnými cezhraničnými ohrozeniami zdravia.

Article 9 EU GDPR "Processing of special categories of personal data"

Článok 23 ods. 2 nariadenia GDPR umožňuje členským štátom zaviesť legislatívne opatrenia v zmysle **zabezpečenie verejnej bezpečnosti**, ktoré musia spĺňať ustanovenia uvedené v osobitnom odseku.

Takéto legislatívne ustanovenie musí okrem iného obsahovať informácie o rozsahu a kategórii osobných údajov, účel ich spracovania, záruku na zabránenie nezákonného zneužitia, prístupu a prevodu dát, špecifikovať kontrolóra, ale aj riziká pre práva a slobody dotknutých osôb.

Article 23 EU GDPR "Restriction"